УДК 004.056.53

А.В. Кий, Я.М. Копчак, И.Б. Саенко, А.В. Козленко

ДИНАМИЧЕСКОЕ УПРАВЛЕНИЕ ДОСТУПОМ К ИНФОРМАЦИОННЫМ РЕСУРСАМ В КРИТИЧЕСКИ ВАЖНЫХ ИНФРАСТРУКТУРАХ НА ОСНОВЕ ИНФОРМАЦИОННЫХ ПРОФИЛЕЙ ПОЛЬЗОВАТЕЛЕЙ

Кий А.В., Копчак Я.М., Саенко И.Б., Козленко А.В. **Динамическое управление доступом к информационным ресурсам в критически важных инфраструктурах на основе информационных профилей пользователей.**

Аннотация. В статье рассматривается метод динамического управления доступом к информационным ресурсам в критически важных инфраструктурах, основанных на применении информационных профилей пользователей. На основе анализа особенностей разграничения доступа к информационным ресурсам в критически важных инфраструктурах, предлагаются показатели априорной и контекстной избыточности полномочий пользователя, которые используются в разработанном методе. В разработанном методе применяются марковские модели последовательностей обращений к информационным ресурсам, используемые для построения информационных профилей пользователей, и методы последовательного анализа данных, используемые для контроля соответствия действий пользователей сформированным профилям. Приводится экспериментальная оценка метода.

Ключевые слова: разграничение доступа, несанкционированный доступ, критически важная инфраструктура, информационный профиль пользователя, кумулятивная сумма.

Kiy A.V., Kopchak J.M., Saenko I.B., Kozlenko A.V. **Dynamic access control of information resources in critical infrastructures based on the users' information profiles.**

Abstract. The paper describes a method of dynamically control access to information resources in critical infrastructures, based on the users' information profiles. The indicators of a priori and contextual redundancy of users' rights are offered, which are used in the developed method on the basis of an analysis of the characteristics of differentiation of access to information resources in critical infrastructures,. The method of Markov models to sequences of information resources used for building information users' profiles, and serial data analysis methods, used for verification of conformity of the activities of users formed profiles, are applied. Experimental estimation of the method is provided.

Keywords: access control, unauthorized access, critical infrastructure, user information profile, the cumulative amount.

1. Введение. Критически важные инфраструктуры (КВИ) с высокими требованиями к непрерывности функционирования и защищенности обрабатываемой информации строятся, как правило, по принципу замкнутой функциональной среды, что предполагает ограничение их связи с сетями общего пользования [1]. В этих условиях основными источниками угроз безопасности информации становятся внутренние нарушители. Опасность данных угроз определяется их непредсказуемостью, наличием у пользователя полномочий по доступу к защищае-

мым ресурсам, объективно существующими уязвимостями средств вычислительной техники (ВТ), а также непрерывным совершенствованием средств и способов несанкционированного доступа (НСД).

Как известно, основой системы защиты информации (СЗИ) от НСД является подсистема управления доступом, ключевыми задачами которой являются предотвращение несанкционированного использования защищаемых ресурсов КВИ и предотвращение использования ресурсов неполномочным способом [2]. Первая задача решается с помощью разграничения доступа, в рамках которого пользователи наделяются соответствующими полномочиями по доступу к информационным ресурсам (ИР), и последующего контроля запрашиваемых видов доступа на предмет соответствия предоставленным полномочиям [3]. Вторая задача, в основном, решается организационными мерами. В связи с этим одним из важных направлений дальнейшего совершенствования СЗИ КВИ является разработка высокоэффективных методов управления разграничением доступа к информационным ресурсам для внутренних пользователей.

Целью работы является рассмотрение предлагаемого метода динамического управления доступа к ИР в КВИ, разработанного на основе учета информационных профилей пользователей и обеспечивающего высокую эффективность защиты от угроз безопасности информации со стороны внутренних пользователей.

2. Особенности разграничения доступа к информационным ресурсам в КВИ. К основным особенностям КВИ следует отнести наличие ограниченного числа постоянных пользователей, высокую степень регламентации деятельности пользователей на средствах ВТ установленными правилами выполнения работ, технологическими схемами обработки информации, а также принятой политикой безопасности, которая определяет для каждого пользователя конечные перечни доступных программных средств, доступных информационных ресурсов и соответствующих полномочий по доступу к ним.

Деятельность пользователей КВИ на средствах ВТ также имеет ряд особенностей. Основными из них являются: *структурированность*, заключающаяся в возможности выделения конечных, логически завершенных этапов деятельности — функциональных задач (ФЗ); *иерархичность*, выражающаяся в том, что в каждой задаче могут быть выделены этапы ее выполнения, при этом сама задача может рассматриваться как один из этапов другой задачи; *цикличность*, заключающаяся в периодическом повторении выполняемых задач и их этапов; *устойчивость*, заключающаяся в повторяемости приемов реализации

отдельных задач, что обусловлено наличием у пользователя устойчивых навыков их выполнения, сформировавшихся в процессе регулярной работы на средствах ВТ [4].

В результате каждым пользователем КВИ в ходе выполнения функциональных задач на средствах ВТ реализуется соответствующая типовая схема использования ИР. При этом, действия пользователя, отклоняющиеся от типовой схемы использования информационных ресурсов КВИ, то есть *атипичные действия*, можно рассматривать как попытку или подготовку НСД, даже в том случае, если данные действия в явном виде не нарушают принятую политику безопасности.

Степень свободы пользователя по совершению атипичных действий определяется полнотой реализованного контроля действий пользователя, количеством предоставленных в доступ ИР и полномочиями по доступу к ним, которые, как правило, являются избыточными по отношению к тем функциональным задачам, решение которых пользователи осуществляют на средствах ВТ. При этом следует констатировать наличие как априорной, так и контекстной избыточности.

*Априорная избыточнос*ть характеризует превышение предоставленных пользователю при разграничении доступа полномочий относительно реального объема полномочий, необходимого для решения возложенных на него задач. Наличие априорной избыточности обусловлено следующими факторами: применением типовых (предустановленных) наборов полномочий; сложностью интерпретации заявленных информационных потребностей пользователей типовыми (принятыми в операционной системе) формализованными операциями и правилами предоставления доступа; необходимостью учета дополнительных полномочий для согласованного функционирования программных средств; необходимостью обеспечения высокой доступности информационных ресурсов, обусловленной жесткими требованиями к непрерывности функционирования КВИ.

Контекстная избыточность характеризует превышение предоставленного объема полномочий относительно реальных потребностей пользователя в контексте отдельной функциональной задачи. Наличие контекстной избыточности обусловлено тем, что применяемые в КВИ средства управления доступом реализуют статический подход, так как осуществляют управление доступом на основе правил, предварительно заданных на весь период функционирования КВИ. Это приводит к тому, что вне зависимости от текущего содержания деятельности пользователя ему постоянно предоставлен весь объем ранее запланированных полномочий.

В качестве показателей априорной и контекстной избыточности полномочий пользователя могут быть использованы следующие коэффициенты:

$$K_{\text{изб}}^{\text{апр}} = \frac{N_{\text{пред}} - \bigcup_{r=1}^{R} N_{\text{треб}}^{r}}{N_{\text{пред}}}, \quad (1)$$

$$K_{\text{изб},r}^{\text{конт}} = \frac{N_{\text{пред}} - N_{\text{треб}}^{r}}{N_{\text{пред}}}, \quad (2)$$

где $K_{\text{изб}}^{\text{апр}}$ — коэффициент априорной избыточности; $N_{\text{пред}}$ — множество предоставленных пользователю полномочий на этапе разграничения доступа; $K_{\text{изб},r}^{\text{конт}}$ — коэффициент контекстной избыточности при выполнении r-ой ФЗ, $r = \overline{1,R}$; $N_{\text{треб}}^{r}$ — множество полномочий, требуемых пользователю для выполнении *r*-ой ФЗ.

Анализ результатов практической деятельности пользователей КВИ при выполнении ФЗ на средствах ВТ, приведенных в таблице, подтверждает наличие избыточности их полномочий по доступу к ИР. Данные получены с помощью программ *AccessChk* и *Process Monitor*, входящих в состав набора *Sysinternals Suite*[1].

Результаты расчета коэффициента контекстной избыточности для различных типов задач

№ ФЗ	**Тип выполняемой функциональной задачи**	$N_{\text{пред}}$	$N_{\text{треб}}^{r}$	$K_{\text{изб},r}^{\text{конт}}$
1	Анализ исходных данных для решения специальной задачи	180	81	0,55
2	Моделирование вариантов принятия решения	180	117	0,35
3	Разработка планирующих документов	180	45	0,75

Наличие избыточности в предоставленных пользователю полномочиях расширяет его возможности по совершению атипичных действий. Характер зависимости вероятности $P_{\text{атип}}$ совершения пользователем последовательности из $k_{\text{атип}}$ атипичных действий от коэффициента контекстной избыточности $K_{\text{изб}}^{\text{конт}}$ приведен на рис. 1.

[1]Данный набор программ по состоянию на 01.01.2012 доступен на сайте http://technet.microsoft.com/en-us/sysinternals/bb842062.

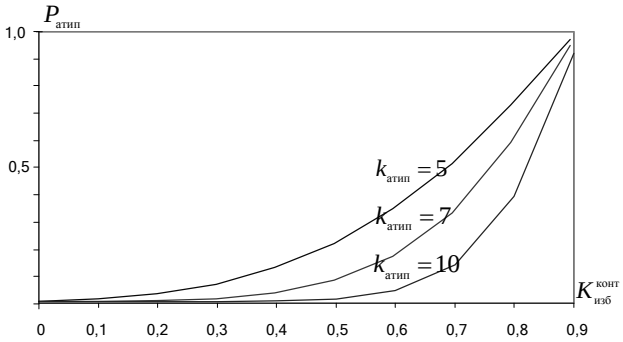

Рис. 1.Зависимость вероятности совершения пользователем последовательности атипичных действий.

Исходя из пессимистичного предположения, что каждое атипичное действие является подготовкой или попыткой НСД, а также с учетом подхода, изложенного в [5], можно установить характер зависимости относительного снижения защищенности КВИ $\partial P_{защ}$ от коэффициента контекстной избыточности $K_{изб}^{конт}$ (рис. 2).

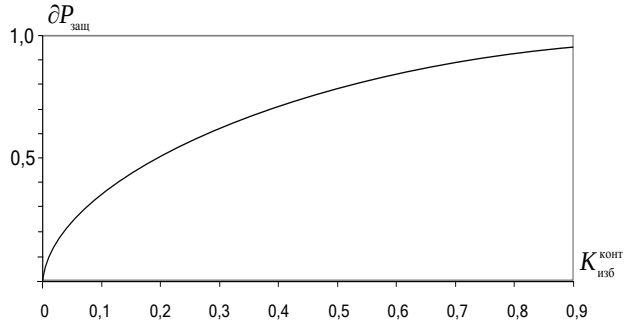

Рис. 2. Зависимости относительного снижения защищенности КВИ от коэффициента контекстной избыточности.

Таким образом, одним из актуальных направлений совершенствования системы управления доступом КВИ является разработка методов динамического управления доступом, обеспечивающих снижение избыточности в предоставленных пользователю полномочиях и предотвращение использования предоставленных ИР неполномочным способом.

3. Анализ известных подходов к динамическому управлению доступом. В настоящее время известен ряд подходов динамического управления доступом к ресурсам АС. В связи с этим целесообразно провести анализ данных подходов на предмет возможности их применения в составе системы защиты информации КВИ.

RSBAC (*rule set based access control*) — контроль доступа, основанный на множестве правил [6]. *RSBAC* имеет модульную структуру. Окончательное решение о предоставлении доступа или отказе в нем получается как суммарное после «обсуждения» этого вопроса всеми модулями. Вместе с тем, конфликты решений, принятых модулями, могут привести к временной блокировке доступа к данным, а в отдельных случаях — и к их потере.

Flexible mandatory access control architecture (*FLASK*) — подход, реализующий гибкую архитектуру принудительного контроля доступа, использующую развитый язык описания конфигураций политики безопасности [7]. В данном методе политика безопасности определяет набор доменов и типов, а также набор ролей. Для каждой роли задается набор доменов, в которых допускается работа с этой ролью. По мере выполнения программ происходит автоматическое перемещение ролей в другие домены для обеспечения изменения привилегий. Выбор домена, в который должно быть произведено перемещение, осуществляется на основе типа запускаемой программы с учетом текущего домена. Недостатком данного метода является сложность его предварительной настройки, а также сложность интерпретации заявленных потребностей пользователей в формализованные операции и правила.

При *динамическом ролевом управлении доступом* права доступа даются пользователю посредством ролевого набора, определяющего список ролей, на которые пользователь может быть авторизован для выполнения различных ФЗ [8]. При этом возможно как совместное использование ролей в течение сеанса работы, так и их перенастройка в случае взаимоисключающих ролей. К недостаткам данного метода относится отсутствие возможности учета изменяющихся условий функционирования КВИ в процессе принятия решения о предоставлении доступа.

Модель управления доступом «*Китайская стена*» реализует динамическое изменение прав доступа на основе множества правил, декларирующих то, что ни один субъект не может получить доступ к объекту по некорректную сторону стены [3]. Основой политики «Китайской стены» является утверждение о том, что субъект может получить доступ к информации, не входящей в конфликт с любой инфор-

мацией, к которой он имел доступ до этого. Определяются классы конфликтов интересов, включающие в себя некоторые информационные ресурсы. Если субъект получил доступ к одному из этих ресурсов, то ему запрещается доступ к ресурсам, входящим в тот же класс конфликта интересов. При этом изначально субъект может получить доступ к любому информационному ресурсу по своему выбору, что существенно ограничивает применение модели для КВИ.

Context Based Access Control (*CBAC*) — динамическое управление доступом на основе формально заданных правил. Этот метод заключается в назначении атрибутов доступа (чтение, вставка, удаление, обновление, управление и т. д.) объектам доступа в зависимости от предыдущих запросов пользователя [9]. Механизм *CBAC* имеет возможность интеллектуального контроля доступа к объектам, основанного на информации об уже используемых в ходе сеанса работы пользователя объектах доступа. Чтобы получить доступ к объекту на основе *CBAC,* пользователь должен выполнить определенную последовательность действий (обратиться и получить доступ к определенной совокупности объектов, закрыть определенные приложения). Система «знает» необходимые шаги, которые должен совершить субъект для доступа к объекту, и проверяет, что они были соблюдены. Иначе в доступе будет отказано. Недостатком этого метода является учет только предыстории запросов пользователя, что не обеспечивает возможность учета значений ряда информативных параметров, характеризующих текущее состояние безопасности.

Таким образом, проведенный анализ показал, что известные подходы обладают рядом существенных недостатков, ограничивающих их применение в КВИ. Этим определяется необходимость разработки и реализации метода динамического управления доступом к информационным ресурсам КВИ на основе применения профилей действий пользователей.

4. Метод динамического управления доступом на основе информационных профилей пользователей. Предлагаемый подход заключается в предварительном формировании, путем наблюдения за работой пользователя КВИ, его иерархического информационного профиля (ИП), элементы которого характеризуют подмножество ИР и порядок их использования в ходе выполнения пользователем различных ФЗ. В дальнейшем сформированный профиль применяется для оценки степени атипичности действий пользователя. Возможность оценки обеспечивается иерархической структурой профиля, каждый уровень которого с соответствующей степенью детализации описывает

все множество типовых схем использования ИР пользователем в процессе выполнения различных ФЗ. Решение о предоставлении доступа пользователя к ИР принимается в зависимости от текущих требований к защищенности информации в КВИ.

Информативными признаками, отражающими деятельность пользователя КВИ на средствах ВТ, являются события доступа, каждое из которых представляет собой комбинацию запрашиваемого вида доступа и идентификатора информационного ресурса. Данные события доступны для сбора и анализа в рамках подсистемы аудита.

Вероятностный характер действий пользователей при выполнении ФЗ, дискретность протекания процессов в вычислительной среде, а также ряд других факторов обуславливают использование для описания работы пользователя аппарата марковских цепей [10]. Поэтому структуру иерархического ИП пользователя можно представить в следующем виде:

$$PI = \left\{ \Lambda_{r,\beta} \right\}, r = \overline{1, R_\beta}, \ \beta = \overline{1, B}, \qquad (3)$$

где PI — иерархический ИП пользователя, $\Lambda_{r,\beta} = [N_r, K_r]$ — элемент ИП; N_r — матрица вероятностей переходов событий доступа, K_r — вектор начального распределения вероятностей событий доступа, B — количество уровней иерархии ИП, R_β — множество элементов ИП на β-ом уровне иерархии ИП.

Формирование иерархического ИП пользователя осуществляется путем наблюдения за работой пользователя, выделения и накопления фрагментов, представляющих собой последовательности событий доступа, соответствующие выполнению пользователем той или иной ФЗ или ее этапа. Выделение фрагментов деятельности пользователя (ФДП) связано с изменением списка активных программных средств. Все множество накопленных ФДП разбивается на множество классов, каждый из которых содержит однородные в смысле близости переходных вероятностей событий доступа фрагменты. Для классификации ФДП применен дивизимный алгоритм кластеризации [11]. Общая последовательность разбиений ограничивается отсечением разбиений с неинформативными классами. В качестве эталона для каждого класса принимается матрица вероятностей переходов, соответствующая его центру тяжести. По завершении кластер-процедуры ИП представляет собой иерархически упорядоченное множество классов ФДП:

$$\Phi = \{\Phi_{s,\beta}\},\ s = \overline{1, S_\beta},\ \beta = \overline{1, B}, \quad (4)$$

где $\Phi_{s,\beta} = \{a_s\}$, $a = \overline{1, A_s}$ — s-й класс ФДП, $\sum_{s=1}^{S} A_s = A$ – множество ФДП, полученных в результате наблюдения за работой пользователя, β — уровень иерархии ИП.

Оценивание степени атипичности наблюдаемых действий пользователя осуществляется путем проверки их соответствия различным уровням иерархического ИП. Наибольшее значение уровня иерархии ИП, элементам которого соответствуют наблюдаемые действия пользователя, принимается за оценку их атипичности. Меньшее значение полученной оценки соответствует большей степени атипичности действий пользователя.

Принятие решения о соответствии действий пользователя β-му уровню иерархии ИП осуществляется путем проверки соотнесения наблюдаемой последовательности событий доступа $\eta_1, \eta_2, \eta_3, \ldots, \eta_\gamma$, зафиксированной в последовательные моменты времени $t_1, t_2, t_3, \ldots, t_\gamma$, с описаниями s-х классов ФДП β-го уровня ИП. При этом решающая функция имеет вид:

$$F\left(\eta_1, \eta_2, \eta_3, \ldots, \eta_\gamma \middle| \Lambda_{s,\beta}\right) = \begin{cases} 1, \text{ если } \eta_1, \eta_2, \eta_3, \ldots, \eta_\gamma \approx \Lambda_{s,\beta}, \\ 0, \text{ в противном случае,} \end{cases} \quad (5)$$

где γ — длина контекста контроля.

Под *контекстом контроля* понимается последовательность событий доступа фиксированной длины, используемая для проверки соответствия наблюдаемых действий пользователя классам ФДП β-го уровня ИП. Введение контекста контроля позволяет рассматривать решаемую задачу в аспекте последовательного анализа, то есть как задачу скорейшего обнаружения момента изменения свойств временного ряда (разладки).

В целях обеспечения минимального времени обнаружения разладки применен алгоритм *кумулятивных сумм* (КС) [12]. Применение данного алгоритма заключается в проверке всех пар гипотез, для чего рассчитываются значения частных КС s-го класса ФДП в отношении других классов β-го уровня в соответствии со следующими выражениями:

$$\lambda_{s,i}(t_{\varsigma+1}) = \omega\left(\Delta\lambda_{s,i}(t_{\varsigma+1})\right)\times\left(\lambda_{s,i}(t_{\varsigma}) + \Delta\lambda_{s,i}(t_{\varsigma+1})\right), i = \overline{1,S}_{\beta},\ i \neq s \qquad (6)$$

,

$$\Delta\lambda_{s,i}(t_{\varsigma}) = \ln\frac{P(\eta_{\varsigma-n+1}, \eta_{\varsigma-n+2},\ldots,\eta_{\varsigma}\left|\Lambda_{i,\beta}\right.)}{P(\eta_{\varsigma-n+1}, \eta_{\varsigma-n+2},\ldots,\eta_{\varsigma}\left|\Lambda_{s,\beta}\right.)}, \qquad (7)$$

где $\lambda_{s,i}(t_{\varsigma})$ — значение частной КС s-го класса в отношении i-го класса в момент времени t_{ς}, $\omega\left(\Delta\lambda_{s,i}(t_{\varsigma})\right)$ — сингулярная функция, определяемая выражением

$$\omega\left(\Delta\lambda_{s,i}(t_{\varsigma})\right) = \begin{cases} 1, \text{ при } \Delta\lambda_{s,i}(t_{\varsigma}) \geq 0, \\ 0, \text{при } \Delta\lambda_{s,i}(t_{\varsigma}) < 0. \end{cases}, \qquad (8)$$

Критерием принятия решения о несоответствии наблюдаемой последовательности событий доступа s-му классу ФДП является превышение в момент времени $t_{\varsigma} = t^{\text{прев}}$ значений одной из накопленных частных КС некоторой пороговой величины $h_{s,i}$.

Алгоритм КС предполагает, что при наблюдении ранее неизвестной последовательности действий пользователя решение все равно будет выноситься в пользу одного из известных классов. При этом в ряде случаев частные КС могут не превышать допустимых порогов, что в результате приводит к принятию неверного решения.

В связи с этим существует необходимость введения обобщенной КС, рассчитываемой в соответствии со следующим выражением:

$$\lambda_{s,\Sigma}(t_{\varsigma+1}) = \omega\left(\Delta\lambda_{s,\Sigma}(t_{\varsigma+1})\right)\times\left(\lambda_{s,\Sigma}(t_{\varsigma}) + \Delta\lambda_{s,\Sigma}(t_{\varsigma+1})\right), \qquad (9)$$

где $\lambda_{s,\Sigma}(t_{\varsigma+1})$ — значение обобщенной КС для s-го класса, а $\Delta\lambda_{s,\Sigma}\left(t_{\varsigma}\right)$ определяется с помощью следующего выражения:

$$\Delta\lambda_{s,\Sigma}\left(t_{\varsigma}\right) = \frac{\sum_{i=1, i\neq s}^{S}\Delta\lambda_{s,i}\left(t_{\varsigma}\right)}{\sum_{i=1, i\neq s}^{S}\omega\left(\Delta\lambda_{s,i}\left(t_{\varsigma}\right)\right)}. \qquad (10)$$

Таким образом, критерием принятия решения о соответствии наблюдаемой последовательности действий пользователя s-му классу ФДП β-го уровня иерархии ИП является следующее условие:

$$\forall \eta_\varsigma \left| t_\gamma < t_\varsigma \le t_{\gamma+1}\right., \ \exists \Phi_{s,\beta} \left| \left(F\left(\eta_1, \eta_2, \ldots, \eta_\varsigma \left| \Lambda_{s,\beta} \right.\right) = 1 \right), \right. \tag{11}$$

где

$$F\left(\eta_1, \eta_2, \ldots, \eta_\varsigma \left| \Lambda_{s,\beta} \right.\right) = \begin{cases} 0, \text{ если } \left(\exists \lambda_{s,i}(t_\varsigma) \left| \lambda_{s,i}(t_\varsigma) \ge h_{s,i} \right.\right) \vee \\ \left(\lambda_{s,\Sigma}(t_\varsigma) \ge h_{s,\Sigma}\right), \\ 1, \text{ в противном случае.} \end{cases} \tag{12}$$

Наблюдаемая последовательность действий пользователя считается не соответствующей заданному уровню иерархии ИП в случае невыполнения критерия (11) для всех классов данного уровня.

Нахождение значений порогов осуществляется на основании выборки ФДП, полученной в результате наблюдения за работой пользователя. При этом учитываются требования к процессу контроля, задаваемые в виде допустимых значений ошибок первого и второго рода. Выполнение требований на каждом уровне иерархии ИП достигается за счет выбора соответствующего значения длины контекста контроля в соответствии со следующими условиями:

$$L_{\text{конт}} \to \max, K^1_{\text{ош}} \le K^1_{\text{ош доп}}, K^2_{\text{ош}} \le K^2_{\text{ош доп}}, \tag{13}$$

где $L_{\text{конт}} = \gamma$ — длина контекста контроля; $K^1_{\text{ош доп}}$ и $K^2_{\text{ош доп}}$ — допустимые значения коэффициентов ошибок первого и второго рода, соответственно.

При нахождении пороговых значений, в целях снижения вычислительных затрат, расчет значений КС для всех ФДП осуществляется один раз на первом шаге. При других значениях длины контекста вычисление КС осуществляется только для ограниченного множества ФДП, достаточного для проверки условий (13).

Управление доступом пользователя к ИР в КВИ осуществляется путем контроля наблюдаемой последовательности его действий на предмет соответствия в каждый момент времени заданному уровню иерархии ИП. В случае несоответствия действий пользователя заданному уровню доступ к ИР либо блокируется, либо ограничивается в зависимости от принятой в КВИ политики безопасности.

Текущий уровень иерархии ИП, на соответствие которому осуществляется контроль действий пользователя, то есть текущий уровень контроля, может изменяться в процессе функционирования КВИ и определяется требованиями к защищенности процесса обработки информации. Увеличение значения уровня контроля повышает требования к степени соответствия действий пользователя его ИП и сопровождается повышением вероятности необоснованного отказа в досту-

пе, что при отсутствии необходимой технологической дисциплины пользователей может привести к снижению оперативности процесса обработки информации в КВИ. Увеличение значения текущего уровня контроля может быть оправдано, например, в случае выявления неизвестного ранее вида угрозы НСД до момента разработки и применения эффективных мер противодействия.

Результаты экспериментальной оценки разработанного метода динамического управления доступом представлены на рис. 3.

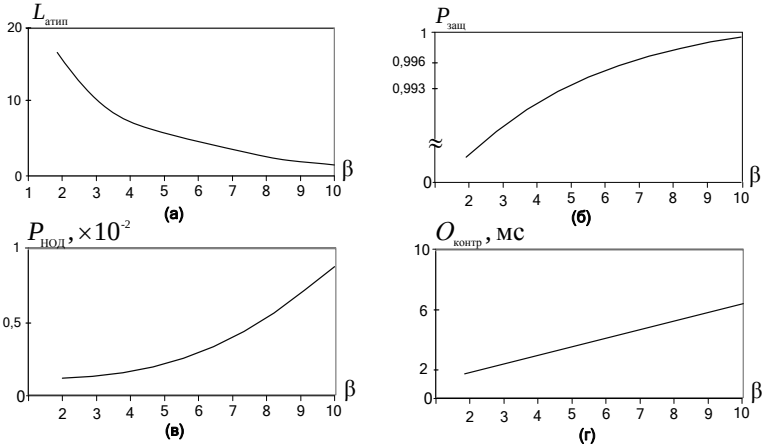

Рис. 3. Результаты экспериментальной оценки метода динамического управления доступа на основе информационных профилей пользователей.

5. Заключение. Приведенные на рисунке зависимости подтверждают утверждение, что увеличение уровня контроля приводит к снижению возможностей пользователя по совершению последовательностей из$L_{атип}$ атипичных действий (рис. 3, *а*). Этим обуславливается повышение вероятности защищенного функционирования$P_{защ}$ КВИ (рис. 3, *б*) и, одновременно с этим, возрастание вероятности необоснованного отказа в доступе $P_{НОД}$ (рис. 3, *в*), а также линейный рост вычислительных затрат (рис. 3, *г*).

Таким образом, предлагаемый метод управления доступом может быть реализован в СЗИ КВИ как дополнительный рубеж защиты, успешно дополняющий возможности традиционных средств разграничения доступа в целях обеспечения требуемой защищенности от угроз безопасности со стороны внутренних пользователей.

Литература

1. *Синецук Ю.И., Филиппов А.Г., Терехин С.Н., Николаев Д.В., Саенко И.Б.* Структурно-логический метод анализа безопасности потенциально опасных объектов // Труды СПИИРАН. 2011. Вып. 2(17). С. 55–69.
2. ГОСТ Р ИСО 7498–2–99. Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Ч. 2. Архитектура защиты информации. М.: Изд-во стандартов, 1999. 39 с.
3. *Корт С. С.* Теоретические основы защиты информации: Учебное пособие. М.: Гелиос АРВ, 2004. 240 с.
4. *Суворова Г. А.* Психология деятельности. М.: ПЕРСЭ, 2003. 176 с.
5. *Вентцель Е.С., Овчаров Л.А.* Теория вероятностей и ее инженерные приложения: Учеб. пособие для втузов. 2-е изд., стер. М.: Высш. шк., 2000. 480 с.
6. Rule Set Based Access Control (RSBAC) for Linux.[электронный ресурс http://rsbac.org].
7. *Кокер Ф.* Введение в SeLinux: новый SeLinux. [электронный ресурс http://www.linuxcenter.ru/lib/articles/system/intro_selinux.phtml].
8. *Бочков М.В., Горюнов М.Н.* Модель динамического ролевого управления доступом на основе оценки лояльности поведения пользователя // Вестник компьютерных и информационных технологий, №04, 2007.
9. *Surhone L.M., Tennoe M.T., Henssonow S.F.* Context-Based Access Control.S.I.: Betascript Publ. 2010. 152 p.
10. *Тихонов В.И., Миронов М.А.* Марковские процессы. М.: Советское радио, 1977. 488 с.
11. *Айвазян С.А., Бухштабер В.М., Енюков И.С., Мешалкин Л.Д.* Прикладная статистика: Классификация и снижение размерности: Справ. изд. М.: Финансы и статистика, 1989.607 с.
12. *Никифоров И.В.* Последовательное обнаружение свойств временных рядов. М.: Наука, 1983. 200 с.

Кий Андрей Вячеславович — адъюнкт Военной академии связи. Область научных интересов: разграничение доступа к информации. Число научных публикаций — 13. kiyarmy@rambler.ru; Военная академия связи, Тихорецкий проспект, 3, Санкт-Петербург, 194064, РФ; р.т. +7(812)247-9842. Научный руководитель — Я.М. Копчак.

Kiy Andrey Vyacheslavovich — post-graduate student, Military academy of communications. Research interests: access control of information. The number of publications — 13.kiyarmy@yandex.ru; Military academy of communications, Tihoretskiy broad street, 3, St. Petersburg, 194064, Russia; office phone +7(812)247-9842. Scientific adviser — Y.M. Kopchak.

Копчак Ян Миланович — канд. техн. наук, заместитель начальника учебного отдела Военной академии связи. Область научных интересов: разграничение доступа к информации, программирование, разработка комплексов программ. Число научных публикаций — 50. ymkoph@yandex.ru; Военная академия связи, Тихорецкий проспект, 3, Санкт-Петербург, 194064, РФ; р.т. +7(812)247-9842. Научный консультант — И.Б. Саенко.

Kopchak Yan Milanovich — PhD, deputy head of educational department of Military academy of communications. Research interests: access control of information, programming, software complex development. The number of publications — 50.ymkoph@yandex.ru; Military

academy of communications, Tihoretskiy broad street, 3, St. Petersburg, 194064, Russia; office phone +7(812)247-9842. Scientific consultant — I.B. Saenko.

Саенко Игорь Борисович — д-р техн. наук, проф.; ведущий научный сотрудник лаборатории проблем компьютерной безопасности СПИИРАН. Область научных интересов: автоматизированные информационные системы, информационная безопасность. Число научных публикаций —250. ibsaen@mail.ru; СПИИРАН, 14-я линия В.О., 39, Санкт-Петербург, 199178, РФ; р.т. +7(812)328-2642, факс +7(812)328-4450.

Saenko Igor Borisovich — Ph.D., Doctor of Technical Sciences, professor; leading research scientist of laboratory of computer network security, SPIIRAS. Research interests: automated information systems, information security. The number of publications — 250. ibsaen@mail.ru; SPIIRAS, 14-th line, 39, St. Petersburg, 199178, Russia; office phone +7(812) 328-2642, fax +7(812)328-4450.

Козленко Андрей Владимирович — адъюнкт Военной академии связи. Область научных интересов: оценивание и контроль защищенности информации, программирование, разработка комплексов программ. Число научных публикаций — 23. et-ak@yandex.ru; Военная академия связи, Тихорецкий проспект, 3, Санкт-Петербург, 194064, РФ; р.т. +7(812)247-9842. Научный руководитель — В.С. Авраменко.

Kozlenko Andrey Vladimirovich — post-graduate student, Military academy of communications. Research interests: the information security estimation and control, programming, software complex development. The number of publications — 23. et-ak@yandex.ru; Military academy of communications, Tihoretskiy broad street, 3, St. Petersburg, 194064, Russia; office phone +7(812)247-9842. Scientific adviser — V.S. Avramenko.

Рекомендовано лабораторией проблем компьютерной безопасности, заведующий лабораторией Котенко И.В., д-р техн. наук, проф.
Статья поступила в редакцию 05.03.2012.

РЕФЕРАТ

Кий А.В., Копчак Я.М., Саенко И.Б., Козленко А.В. **Динамическое управление доступом к информационным ресурсам в критически важных инфраструктурах на основе информационных профилей пользователей.**

Целью работы является рассмотрение предлагаемого метода динамического управления доступом к информационным ресурсам в критически важных инфраструктурах, разработанного на основе учета информационных профилей пользователей и обеспечивающего высокую эффективность защиты от угроз безопасности информации со стороны внутренних пользователей.

Проведенный анализ особенностей разграничения доступа к информационным ресурсам в критически важных инфраструктурах позволил выделить и определить показатели априорной и контекстной избыточности полномочий пользователя.

Проведенный анализ известных подходов к динамическому управлению доступом показал, что они обладают рядом существенных недостатков, ограничивающих их применение, и определил разработку и реализацию метода динамического управления доступом на основе применения профилей действий пользователей как перспективное направление в обеспечении информационной безопасности критически важных инфраструктур.

Дана количественная оценка введенных показателей априорной и контекстной избыточности для различных типов задач, решаемых в критически важных инфраструктурах. Результаты проведенной оценки, а также известных подходов к управлению доступом к элементам критических инфраструктур позволили обосновать необходимость разработки метода динамического управления доступом к информационным ресурсам на основе информационных профилей пользователей.

В разработанном методе динамического управления доступом применяются марковские модели последовательностей обращений к информационным ресурсам, используемые для построения информационных профилей пользователей, и методы последовательного анализа данных, используемые для контроля соответствия действий пользователей сформированным профилям. Решающее правило для принятия решения о доступе пользователя к информационному ресурсу осуществляется на основе решения задачи скорейшего обнаружения момента изменения свойств временного ряда с использованием усовершенствованного алгоритма кумулятивных сумм.

Проведенная экспериментальная оценка показала, что предлагаемый метод управления доступом может быть реализован в системах защиты информации критически важной инфраструктуры как дополнительный рубеж защиты, успешно дополняющий возможности традиционных средств разграничения доступа в целях обеспечения требуемой защищенности от угроз безопасности со стороны внутренних пользователей.

SUMMARY

Kiy A.V., Kopchak J.M., Saenko I.B., Kozlenko A.V. **Dynamic access control of information resources in critical infrastructures based on the users' information profiles.**

Purpose of the work is the consideration of the proposed method of dynamically control access to information resources in critical infrastructures, developed on the basis of the information about user's profiles which provides the high efficiency of protection against threats to information security by internal users.

The analysis of features of the access to information resources in critical infrastructures has selected and identified the indicators of a priori and contextual redundancy user rights.

The analysis of known approaches to dynamic access control showed that they have a number of significant deficiencies that limit their use, and defined the development and implementation of the method of dynamic access control based on user activity profile as a promising direction to ensure information security of critical infrastructures.

Quantification of the indicators of a priori and imposed content redundancy for different types of tasks carried out in critical infrastructures is presented. The results of the evaluation, as well as the well-known approaches to the management of access to the elements of critical infrastructure made it possible to justify a method of dynamically access control to information resources based on user information profile.

The method of dynamic access controls applies Markov model sequences of calls to the information resources used to build the user information profiles, and serial data analysis methods, used for verification of conformity of the users activities to formed profiles. The crucial rule enabling the user's access to the information resource is accessed through the early detection of the change of properties of time series with the use of an improved algorithm of the cumulative amounts.

An experimental evaluation showed that the proposed method of access control can be implemented in systems of information protection of critical infrastructures as an additional line of defense successfully complementing traditional means of access in order to ensure the requisite protection against security threats from internal users.