boşluqdan aktiv şəkildə istifadə edilə biləcəyini təxmin etmək üçün istifadə edilə bilər və bu verilənlərdən istifadə edərək bərpa planları tərtib edə bilir.

Güclü hesabatdan istifadə edərək qərarların idarəedilməsi: Risk qiymətləndirmə proseduru başa çatdıqdan sonra nəticələr rəsmi hesabat formatında sənədləşdirilməlidir. Bu hesabat rəhbərliyə, missiya sahiblərinə siyasət, prosedur, büdcə və sistem əməliyyat və idarəetmə dəyişiklikləri ilə bağlı qərar qəbul etməkdə kömək edəcəkdir. Risk qiymətləndirməsi rekursiv bir prosedur olduğundan bu hazırlanan son hesabat, risk qiymətləndirmə prosedurunun növbəti dövrü üçün təklif olunan freymvörk üzrə 1-ci mərhələnin girişi kimi istifadə ediləcəkdir.

Nəticə: Universitetin şəbəkə mühiti daim genişlənir, yenilənir, komponentləri dəyişdirilir və proqram tətbiqetmələri yeni versiyaları ilə əvəzlənir və ya yenilənir. Bu dəyişikliklər yeni risklərin ortaya çıxacağını və əvvəllər azaldılmış risklərin yenidən problem ola biləcəyini göstərir. Beləliklə, risk idarəçiliyi davam edir və inkişaf edir. Bununla da daha yaxşı təcrübəni və davam edən bir risk qiymətləndirmə modeli və qiymətləndirmə ehtiyacı vurğulanır.

**Ədəbiyyat**

1. C. Alberts, and A. Dorofee, “An Introduction to the OCTAVE Method. Software Engineering Institute”, Carnegie Mellon University, USA, 2010.

2. Guide for Applying the Risk Management Framework to Federal Information Systems, U.S. Department of Commerce, February 2010.

## ОЦЕНКА РИСКОВ БЕЗОПАСНОСТИ ДАННЫХ В КОМПЬЮТЕРНОЙ СЕТЕВОЙ СРЕДЕ УНИВЕРСИТЕТА

***Ключевые слова:*** *Риск, сеть, фреймворк, безопасность, система.*

**Резюме:** в этом тезисе рассматриваются вопросы реализации контроля безопасности в неправильных точках в среде компьютерных сетей университета, растрата ресурсов, причины, которые могут сделать университет уязвимым для непредвиденных угроз, а также причины, направленные на осознание слабых мест в постоянно меняющейся и трудно организованной среде университета. Также был рассмотрен принцип работы фреймворка, позволяющий понять риски безопасности в высших учебных заведениях и количественно измерить уровень риска.

## ASSESSMENT OF DATA SECURITY RISKS IN THE COMPUTER NETWORK ENVIRONMENT OF THE UNIVERSITY

***Keywords:*** *Risk, network, framevork, security, system.*

**Summary:** In this thesis, the implementation of security controls at the wrong points in the computer network environment of the University, wasted resources, reasons that may make the University vulnerable to unexpected threats, and reasons aimed at the awareness of weak points in the continuously changing and difficult organized university environment were investigated. The principle of work of framework in order to quantify the level of risk and to understand the safety risks in higher education institutions has also been considered.

## РАЗРАБОТКА МОДЕЛИ АВТОМАТИЗАЦИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**Джафарова Шалала Мехти гызы**

*Сумгаитский государственный университет, Сумгаит, Азербайджан*

*salala.cafarova@mail.ru*

***Ключевые слова:*** *безопасность, облако, автоматизация, моделирование, сеть Петри, нечеткий*

**Резюме:** В наше время облачные сервисы с большим объемом вычислений и памяти широко используются для решения сложных проблем. В этом случае пользователям, работающим в разных местах, выгоднее пользоваться услугами облачной системы. По этой причине необходимо разработать алгоритм защиты безопасности системы. Предложение или разработка таких алгоритмов должны быть инструментом повышения устойчивости к потенциальным сбоям. В данной работе было предложено создать автоматизированную систему моделирования информационной безопасности в облачных технологиях с использованием сети Петри (СП).

В настоящее время во всем мире ведутся интенсивные исследования по эффективному использованию вычислительных ресурсов и ресурсов памяти с помощью облачных технологий. На

основе этой технологии актуально эффективное использование больших информационных ресурсов в неопределенной среде среди пользователей сети и моделирование их безопасности [1].

В облачных сервисах используются различные устройства моделирования для обеспечения и защиты защищенных данных. Таким образом, больше использовались конечные автоматы, логические и продукционные модели, семантика и дригие. Однако по сравнению с этими моделями СП считается более универсальным. Это связано с тем, что исследуемая информация моделируется элементами СП и за ее пределами безопасность создается путем анализа основных свойств.

В результате моделирования определено, что любая ситуация вызвана нежелательным вмешательством в данные. На основании этого результата определяется, какие действия предпринимаются после разрешения ситуации. Затем определяются достаточные или недостаточные случаи созданной системы. Из-за отсутствия абсолютной концепции процесса и однозначной последовательности выполнения в компьютере, его анализ причинно-следственных связей в различных процессах ускоряется, независимо от системы и ее характера [2].

Любой пользователь пытается получить доступ к системе, вводя свой пароль. По позициям и ссылкам СП можно определить, правильно ли был введен пароль пользователя. В этом случае, если пароль вводит реальный пользователь, система будет разблокирована для использования. Однако, если пароль введен неверно, т.е. была предпринята попытка помешать ему каким-либо злоумышленником, то, естественно, в этом случае переход не происходит и система не объявляется открытой для пользователя. Таким образом, СП можно использовать для создания автоматизированной системы моделирования информационной безопасности в облачном сервисе.

Модель информационной безопасности в облачных технологиях была разработана, как показано на рисунке 1. Здесь короткие записи предоставляют информацию о системе в открытом состоянии, почте в открытом состоянии, системе в закрытом состоянии, почте в закрытом состоянии, правильном вводе пароля и неправильном вводе пароля [3].

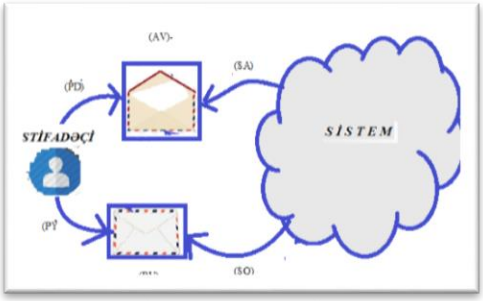


Рисунок 1. Модель информационной безопасности в облачных технологиях

В облачных технологиях бизнес-деятельность определяется в соответствии со схемой автоматизации информационной безопасности. Разработанная нечеткая модель информационной деятельности описывается в виде нечеткой алгебры СП. В этом случае определяются позиции нечеткого алгебраического СП, количество переходов и функции ввода-вывода каждой позиции, перехода.

Описание нечеткой алгебры приведено ниже:

$$D=(P \cup F,\ T,\ A,\ V,\ \mu_0{}^R),$$

где $P=\{p_1,p_2,\ldots,p_n\}$– позиции типа $p$, $F=\{f_1,f_2,\ldots,f_m\}$ – позиции типа $f$, $T=\{t_1,t_2,\ldots,t_r\}$– переходы; $A$- заданный конечный алфавит. $V:[(P \cup F)\times T]\cup[T\times(P \cup F)]\rightarrow A^*$- представляет собой описание отмеченных дуг, соединяющих позиции со звеньями и звеньев с позициями; $\mu_0{}^R:P\cup F \rightarrow A^* \times [0,1]$ $\ell$ - $A^*$ - указывает начальную разметку позиций слов, $A^*$ - $A$ представляет собой свободный моноид и $\ell=card\ X^f(a),\ a\in P \cup F$ [4].

Такое описание показывает, что нечеткие алгебраические пересечения СП зависят от положения их входов и выходов в конфликтной ситуации. Другими словами, если пересечение наборов входных и выходных позиций переходов $t_1$ и $t_2$, соответственно, является пустым набором, то эти переходы не конфликтуют. Если переходы $t_1$ и $t_2$, конфликтуют на выходе, т.е. $a\in P \cup F$ условно удовлетворяется и $V(t_1,a)=S_1$; $V(t_2,a)=S_2$; $S_1 \neq S_2$; $S_1$; Для $S_1$, приведенное здесь $S_2 \in A^*$ - представляет собой операцию конкатенации. Такое описание показывает, что нечеткие алгебраические пересечения СП зависят от положения их входов и выходов в конфликтной ситуации.

Разработаны модель и алгоритм анализа автоматизации деятельности облачных технологий в виде нечеткой алгебраической СП. Этот алгоритм обеспечивает эффективное преобразование внешних данных во внутренний формат, представление структуры в удобной форме и автоматическое обнаружение тупиковых ситуаций.

Последовательность переходов, заданная в начальной разметке $\mu_0$, определяется как $\varphi = (t_3\ t_2\ t_1\ t_4)$ на основе сформированного алгоритма.

На основе полученных результатов построена граф-схема модели информационной активности в облачных технологиях.

**Литература**

1. Каретников, А.В. Безопасность облачных вычислений. Проблемы и перспективы / А.В. Каретников, Д.П. Зегжда // Журнал "Проблемы информационной безопасности. Компьютерные системы". - СПб.: 2011, № 4, с. 7-17.

2. Джафарова Ш.М. Разработка модели информационной безопасности с применением продукционной модели. // Вестник Дагестанского государственного технического университета. Технические науки. Том 48, №3, 2021, с. 68-72.

3. S.M.Jafarova. Information security analysis algorithm in cloud technology.// Scientific and Practical Cyber Security Journal (SPCSJ) 4(4): 1-4 ISSN 2587-4667 Scientific Cyber Security Association (SCSA), Vol 4, №4, Georgia, 2020, p.1-4

4. S.M.Jafarova. One approach to information security in cloud services.// Global Journal of Applied Sciences and Technology ISSN: 2694-3840, USA, Vol. 3 Issue 3, 2021, İmpact Factor: 2.6, p.1-3.

## İNFORMASİYA TƏHLÜKƏSİZLİYİNİN AVTOMATLAŞDIRILMASI MODELİNİN İŞLƏNMƏSİ

***Açar sözlər.*** *təhlükəsizlik, bulud, avtomatlaşdırma, modelləşdirmə, Petri şəbəkəsi, qeyri-səlis.*

**Xülasə:** Müasir dövürdə mürəkkəb məsələlərin həlli üçün böyük həcmdə hesablama və yaddaşa malik bulud servisindən geniş istifadə olunur. Bu zaman müxtəlif yerlərdə fəaliyyət göstərən istifadəçilərin bulud sistemi xidmətlərindən istifadə etməsi daha da sərfəli hesab olunur. Bu səbəbdən də sistemin təhlükəsizliyinin qorunması alqoritmi işlənib hazırlanmalıdır. Belə alqoritmlərin təklif olunması və ya işlənilməsi yarana biləcək nasazlığa davamlılığın artırılması üçün bir vasitə olmalıdır. Bu işdə Petri şəbəkəsindən (PŞ) istifadə olunmaqla, bulud texnologiyalarında informasiya təhlükəsizliyinin modelləşdirilməsi üçün avtomatlaşdırlmış bir sistemin yaradılması təklif olunmuşdur.

## DEVELOPMENT OF INFORMATION SECURITY AUTOMATION MODEL

***Keywords:*** *security, cloud, automation, modeling, Petri network, fuzzy*

***Summary:*** In modern times, cloud services with a large amount of computing and memory are widely used to solve complex problems. In this case, it is more profitable for users operating in different places to use the services of the cloud system. For this reason, an algorithm for protecting the security of the system must be developed. Proposing or developing such algorithms should be a tool to increase the resilience to potential failures. In this study, it was proposed to create an automated system for modeling information security in cloud technologies using the Petri network (PN).

## TV PARLAQLIQ SİQNALININ KVANTLANMASI ZAMANI YARANAN MƏHDUDLAMA KÜYLƏRİNİN AZALDILMASI

**Məmmədov İsa Rəhman oğlu, Layıcov Mübariz Elşad oğlu,**
**Nərimanlı Murad Tərlan oğlu**
*Azərbaycan Dövlət Neft və Sənaye Universiteti, Bakı, Azərbaycan*
*mubarizlaicov@gmail.com*

***Açar sözlər:*** *TV parlaqlıq siqnalı, parlaqlıq siqnalının kvantlanması, məhdudlama küyləri, məhdudlama küylərinin azaldılması.*

**Xülasə:** Tezisdə TV parlaqlıq siqnalının kvantlanması zamanı yaranan məhdudlama küylərinin azaldılması, yaranan küylərin hesablanması və bu küylərin minimum dərəcəyə salınması yolları göstərilmişdir. Parlaqlıq siqnalının kvantlanması zamanı tez-tez bu küylərin yaranması problemləri ilə qarşılaşırıq. Buna görə də bu problemin həll olunması önəm kəsb etmişdir və bunun edilməsi üsulları, onun